Opening Statement
Chairman Tom Davis
"Implementing the SAFETY Act: Advancing New Technologies for Homeland Security"
October 17, 2003

Good morning. A quorum being present, the Committee on Government Reform will come to order. I would like to welcome everyone to today's hearing on the implementation of the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002. The private sector is an important partner in providing for the security of the homeland. To ensure that private sellers, manufacturers and service providers contribute to homeland security by developing potentially life-saving technologies without having to fear crippling or frivolous lawsuits, the government needs to provide litigation and risk management frameworks to adequately prepare for a terrorist attack.

As part of the Homeland Security Act of 2002, Public Law 107-296, Congress enacted the SAFETY Act to provide incentives for the development and deployment of anti-terrorism technologies by creating systems of "risk management" and "litigation management." The SAFETY Act seeks to ensure that the threat of liability does not deter manufacturers or sellers of anti-terrorism technologies from developing and commercializing technologies that could save lives. The Act creates certain frameworks for "claims arising out of, relating to, or resulting from an act of terrorism" where qualified anti-terrorism technologies are deployed. The Act does not limit liability for harms caused by anti-terrorism technologies when no act of terrorism has occurred.

The SAFETY Act directs the Department of Homeland Security to adopt regulations to implement the liability protections conferred by the Act for Qualified Anti-Terrorism Technologies. Under the statute, these qualified technologies would receive several protections, including:

- Limiting lawsuits filed under the Act to Federal courts;
- Prohibiting a plaintiff from recovering punitive damages, but permitting recovery of non-economic damages, such as damages for physical and emotional pain; and
- Reducing any recovery from the seller by the amount of any collateral sources, such as insurance payments.

Some technologies that qualify under the Act may also qualify for a rebuttable "government contractor defense." The "government contractor defense" could provide sellers and manufacturers immunity from product liability altogether when the qualified technology is deployed for the purposes of defending against or responding to a terrorist act.

Under the Act, DHS can certify that the seller or manufacturer will receive this rebuttable defense if DHS determines that the technology will perform as intended, conforms to the seller's specifications, and is safe for use as intended. But the defense will not protect sellers and manufacturers against charges of fraud or willful misconduct. The Act requires DHS to adopt

rules to implement the protections in the Act. The timely adoption and implementation of those rules is the reason for our hearing today.

On July 11, 2003, DHS announced draft regulations implementing the SAFETY Act that were published in the *Federal Register* for public comment. Over forty private firms and private sector associations submitted comments. An interim final rule has been released to the public.

By passing the SAFETY Act, Congress acted quickly to resolve uncertainty over liability concerns so that the full power of American technology could be unleashed in the war on terrorism. We gave DHS responsibility to develop a transparent process to accomplish these objectives. It is imperative that DHS begin qualifying existing and new technologies so they can be placed in the hands of those who need them now, especially for those high priority homeland security procurements that have been "on hold" pending the qualification of anti-terrorism technology already selected for use.

For its part, when DHS issued the draft regulations in July, it stated it would begin accepting applications for SAFETY Act protections on September 1, 2003. But the actual form to be used for private firms to qualify anti-terrorism technologies was not approved by OMB until this week. Also, the interim final rule was only issued by DHS this week. As a result of these bureaucratic delays, private firms have waited to submit applications until they have seen some finality in the application process and implementing regulations. It is imperative that DHS now mobilize its efforts to accomplish this critical purpose of the SAFETY Act.

In so doing, DHS must identify and implement a clear strategy for prioritizing the many applications it will receive for the qualification of anti-terrorism technologies. Congress did not intend for the SAFETY Act to be used solely as a means for the development of "new" anti-terrorism technologies. While developing new technology is essential, I believe DHS needs to focus on qualifying "existing" anti-terrorism technologies that are ready to be deployed to protect our civilian population. I urge DHS to make as its number one priority the identification, prioritization and qualification of "existing" anti-terrorism technologies that are now being sought by federal and non-federal entities. It is imperative that we protect the highest priority facilities and critical infrastructure in high risk locations.

In addition, DHS must be careful that its implementing regulations and processes are not so complicated that they defeat the very purpose of the SAFETY Act. They should allow for the rapid deployment of anti-terrorism technology necessary to protect the American people, rather than create burdensome red tape and bureaucracy. Wherever possible, decisions regarding the suitability of anti-terrorism technology should rest with those entities charged with the responsibility of acquiring the technology. It is also imperative that DHS adheres to a disciplined time schedule for processing applications.

Through this hearing, the Committee intends to learn about the interim final rule promulgated by DHS and whether the rule effectuates the Congressional intent of the Act. The Committee hopes this open discussion will result in effective implementation of the Act.

We have assembled an impressive group of witnesses to help us understand the statute, the proposed rules, and the private sector concerns about the proposed rules. We will first hear from The Honorable Parney Albright, Assistance Secretary for Plans, Programs, and Budgets of the Department of Homeland Security. Next, we will hear from private sector witnesses: Mr.

Harris Miller, President of the Information Technology Association of America; Mr. Stan Z. Soloway, President of the Professional Services Council; and Mr. John Clerici, representing the U.S. Chamber of Commerce.

I would like to thank all of our witnesses for appearing before the Committee, and I look forward to their testimony.